

REMARKS

The examiner has rejected (or objected to) claim 64 and in the same sentence has referred to claim 23. In the preliminary amendment filed July 13, 2001, applicant cancelled claims 23 and 64 and added a new claim 65.

Claims 1-63 stand rejected under 35 USC 103 over U.S. Patent 5,793,027 and WO 98/44402 (Bramhill). Applicant believes that the examiner did not intend to refer to U.S. Patent 5,793,027, but intended to refer instead to U.S. Patent 5,793,028 (Wagener).

Claims 1-65 have been cancelled and replaced with new claims 66-102. Claims 66, 76, 81, 90, 98 and 102 are independent claims. The new dependent claims correspond to the original claims 2-7, 10-12, 21-24, 29-33, 36-38, 47-52, 55 and 57-63 respectively.

The new claim 66 is based on the original claim 1 and is worded to emphasize the important features that distinguish the invention over the prior art. Claim 66 is now directed to a network system comprising a first computer arrangement and a second computer arrangement. The first computer arrangement is programmed to request data from the second computer arrangement. In response to this request, the second computer arrangement delivers fingerprint software to the first computer arrangement. The fingerprint software is then executed by the first computer arrangement to generate fingerprint data that is substantially unique to the first computer arrangement. The fingerprint data is then returned to the second computer arrangement. Upon receiving the fingerprint data, the second computer arrangement delivers the requested data to the first computer arrangement. Accordingly, a request for data is only completed upon receiving fingerprint data that substantially uniquely identifies the first computer arrangement.

Basis for the revisions made to claim 1 in order to arrive at claim 66 may be found at, for example, page 9, final paragraph and page 10, first paragraph.

The remaining independent claims have been revised in a manner consistent with claim 1. In particular, claim 76 is directed to the first computer arrangement (referred to in claim 76 as a client computer), claim 81 is directed to the second computer arrangement (a server computer arrangement in claim 81), claim 90 is directed to the

method of claim 66, and claim 98 is directed to software of the second computer arrangement.

Support for the revisions made to claims 12 and 38 in order to arrive at claims 75 and 89 may be found at page 10, first paragraph.

Claim 102 is based on claim 12 but is written in independent form.

Wagener describes a verification system comprising a transactionor computer, a transactionee computer and a verifier computer. Each computer of the verification system has a unique public identification code that is publicly available and a unique private identification code known only to the verifier computer and the particular computer to which the code relates.

When a transaction takes place between the transactionor computer and the transactionee computer, the transactionor computer first transmits a transaction request to the transactionee computer (this transaction request may be sent directly or via the verifier computer). The transaction request includes the public identification code of the transactionor computer. In response, the transactionee computer generates a verification request, which is then transmitted to the verifier computer. The verification request includes the private identification code of the transactionee. The verifier computer in turn generates an acknowledgement request, which is transmitted to the transactionor computer. Upon receiving the acknowledgement request, the transactionor computer generates an acknowledge response, which is then sent to the verifier computer. The acknowledgement response includes the private identification code of the transactionor computer. The verifier computer then checks the private identification code of the acknowledgement response in order to verify the identity of the transactionor computer. Upon verification, the verifier computer transmits a verification response to the transactionee computer, and the transaction between the transactionor computer and the transactionee computer proceeds.

With the system described by Wagener, the verifier computer acts as an intermediary between the transactionor computer and the transactionee computer. Since only private identification codes are used for communications to and from the verifier computer, the verifier computer is able to verify the identity of both the

transactionor computer and the transactionee computer prior to a transaction being initiated.

A drawback with the system described by Wagener is that each transactionor computer and each transactionee computer must be registered with the verifier computer before a transaction can take place. In particular, public and private identification codes for each computer must be created and stored at each computer. Moreover, if a private identification code became known to a third party, the third party could operate a fraudulent computer under the guise of a registered computer. It would not then be possible to identify the fraudulent computer.

With the present invention, on the other hand, the identity of a particular computer (a client or requesting computer) can be obtained without prior registration. This is achieved by the means of fingerprint software that is downloaded from a server in response to a transaction request (i.e. the transfer of requested data) and is executed by the client computer. Moreover, the transaction is not completed (i.e. the requested data is not transferred) until such time as fingerprint data generated by the fingerprint software is received by the server. Accordingly, the identity of the client computer can be obtained without any pre-registration or user involvement.

Bramhill describes a copyright protection scheme in which data is securely sent from a server to a client computer in the form of a cryptographically protected data file, referred to in the reference as a BTC file. The client computer includes an applet that decrypts the BTC file such that the protected data may be accessed. However, the applet prevents the unencrypted copy of the data from being copied.

Bramhill describes a particular embodiment (page 16, line 13 to page 17, line 31) in which the identity of the client computer is used to generate an individual cryptographic key specific to that client computer. Data to be transferred from the server to the client computer is then cryptographically protected using the individual cryptographic key for that client computer so as to improve security. However, in order to obtain the individual cryptographic key, the client computer must first be registered with the server. Registration takes place through the use of a program referred to by Bramhill as a dogtag program. The dogtag program is provided on a CD, i.e. a tangible article, that is delivered by a postal service to the

client machine to ensure security. The dogtag program when executed causes a unique machine identification code (MID) to be created. For added security, the dogtag program can only be executed once for registration purposes. The MID is then transferred from the client computer to the server. The server then generates an individual cryptographic key and embeds the key, along with the MID, into an applet which is then downloaded to the client computer where it is stored. This then completes the registration process. When protected data is to be subsequently downloaded from the server, the dogtag program on the client computer generates a new MID and compares this against the MID stored in the applet on the client computer in order to authenticate the client computer. Once authenticated, the data to be downloaded is cryptographically protected by the server using the individual encryption key for that client computer. The cryptographically protected data is then downloaded and decrypted using the applet stored on the client computer during the registration process.

With the system described by Bramhill, a client computer can only be identified following a relatively lengthy registration process. In particular, the software necessary for registration is provided on a CD using a postal service. Furthermore, the registration software, once installed, must remain resident on the client computer in order that the client computer can self-authenticate prior to data retrieval. It is not therefore possible for a registered user to use an alternative computer. Instead, each and every computer to be identified must first be registered.

With the present invention, on the other hand, the identity of a particular client computer can be obtained without prior registration. Moreover, there is no need for the client computer to have software pre-installed prior to data transfer. Instead, fingerprint software is downloaded and executed in response to a request for data to be transferred. The fingerprint data generated by the fingerprint software is then transmitted to the vendor or verification server in order to identify the client computer. In response to receiving the fingerprint data, the requested data is then transferred to the client computer. Accordingly, the identity of the client computer can be obtained without any user involvement. Moreover, since no prior registration or pre-installed software is required, any client


computer capable of downloading and executing the fingerprint software may be readily identified.

Neither Wagener nor Bramhill describe a system in which fingerprint software is downloaded and executed by a client computer in response to a request for data located on a server, and in which the requested data is only delivered to the client computer once fingerprint data (created by the fingerprint software) is received by the server. Accordingly, it is submitted that the invention as defined in claim 66 is not disclosed or suggested by Wagener and Bramhill, whether taken singly or in combination.

The other independent claims are worded in a manner consistent with that of claim 66. Applicant therefore submits that the arguments presented above in support of claim 66 are applicable to the other independent claims also.

In view of the foregoing, it is submitted that all independent claims are patentable. It follows that the dependent claims also are patentable.

Respectfully submitted,



John Smith-Hill  
Reg. No. 27,730

SMITH-HILL & BEDELL, P.C.  
16100 N.W. Cornell Road, Suite 220  
Beaverton, Oregon 97006

Tel. (503) 574-3100  
Fax (503) 574-3197  
Docket: FORR 2276

Certificate of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to the Patent and Trademark Office on the date shown below.



John Smith-Hill

12/16/05  
Date